Distributed Attack Monitoring Scheme for Islanded DC Microgrids

A. J. Gallo, M. S. Turan, P. Nahata, F. Boem, T. Parisini, G. Ferrari-Trecate

Network of physically interconnected Distributed Generation Units (DGUs), $x_{\text{DGU}} = [V_i, I_i, \nu_i]^T$ with physically coupled dynamics:

$$
\begin{align*}
    \dot{V}_i &= \frac{1}{C_i} I_i + \sum_{j \in \Omega_i} \frac{1}{C_{ij}} \left( V_j - V_i \right) - \frac{1}{C_i} I_i + \nu_{\text{physical coupling}} \\
    \dot{I}_i &= \frac{1}{L_i} V_i - \frac{1}{L_i} I_i - \frac{1}{L_i} V_i + \nu_{\text{physical coupling}} \\
    \dot{\nu}_i &= V_{i,\text{ref}} + \Delta V_i - V_i + \nu_{\text{physical coupling}}
\end{align*}
$$

All states measurable: $x_{\text{DGU}} = x_i + \nu_{\text{physical coupling}}$

**Control architecture**
- Decentralized primary control $V_i = K_i x_{\text{DGU}}^m$
- Distributed consensus-based secondary control $\Delta V_i = \sum_{j \in \Omega_i} \left( I_{ij} - I_{ji} \right)$
  - Requires communication network
  - Introduces opportunity for attack over communication network
  - Communicated measurement:
    $$
    x_{\text{DGU}}^m = x_i^m + \phi_j(t)_{\text{attack}}
    $$

**Microgrid Security**

- **Threshold based detection**
  - Residual error bounded by a time-varying threshold:
    - Bound computed from bounds on noise and UIO error stability
    - Upper bounds on noise → absence of false alarms guaranteed by design

- **Detection Properties**
  - An attack is said to be stealthy if it is not detectable.
  - It is sufficient for an attack to satisfy the following for it to be stealthy to the UIO-based detection strategy
    $$
    \left| \int_{T_0}^{t} e_{j,i} \left( t, L_i \right) H_j \phi_j(t, T_0) + T_j \phi_j(t, T_0) - \frac{d}{dt} \left( \int_{0}^{T_0} H_j \phi_j(t, \tau) + T_j \phi_j(t, \tau) \right) \right| = 0
    $$

- **Stealthy Attacks**
  - An attack is guaranteed to be detected by the monitoring scheme if there is a time $t$ at which the following holds for at least one component:
    $$
    \left| \int_{T_0}^{t} e_{j,i} \left( t, L_i \right) H_j \phi_j(t, T_0) + T_j \phi_j(t, T_0) - \frac{d}{dt} \left( \int_{0}^{T_0} H_j \phi_j(t, \tau) + T_j \phi_j(t, \tau) \right) \right| > 2\| \nu \|_{\text{max}}
    $$

- **Simulation Results**
  - State trajectory under constant bias injection attack
  - UIO residuals vs. thresholds
  - Attacks detected

**Future Research Directions**
- Augmented detection scheme with local state estimation
- Distributed watermarking scheme for replay attack detection
- Realistic DGU model and communication network

**Acknowledgements**
The results presented here were presented at ECC 2018: A. J. Gallo, M. S. Turan, P. Nahata, F. Boem, T. Parisini, & G. Ferrari-Trecate “Distributed Cyber-Attack Detection in the Secondary Control of DC Microgrids”. In European Control Conference 2018